



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,769	10/11/2001	Michael C. Dapp	FS-00510 (02890038AA)	7586
181	7590	12/13/2005	EXAMINER	
MILES & STOCKBRIDGE PC 1751 PINNACLE DRIVE SUITE 500 MCLEAN, VA 22102-3833			HENEGHAN, MATTHEW E	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	Application No. 09/973,769	Applicant(s) DAPP, MICHAEL C.	
	Examiner Matthew Heneghan	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 September 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-48 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-48 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 September 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. In response to the previous office action, claim 1 has been amended and claims 25-48 have been added. Claims 1-48 have been examined.

Drawings

2. The drawings were received on 22 September 2005. These drawings are acceptable.

Claim Objections

3. The previous claim objection is withdrawn in view of Applicant's amendment.
4. Claim 44 is objected to because of the following informalities: The term "a third of said digital network node" in line 11 has no meaning in the context of Applicant's disclosure. It is being presumed that the term should read "a third digital network node."
Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

Art Unit: 2134

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 44-48 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 44 claims the deployment of a manger on each node of the network on line

6. Though the specification discloses a plurality of managers on a network, it does not disclose having a manager on each node.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 25-43 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: It is unclear how the first network port in claim 25, the second network port in claim 26, and the two network ports in claim 35 relate to the remainder of the invention. Since all networks inherently have network ports, these limitations are being ignored.

Art Unit: 2134

Claims 27-34 and 36-43 depend from rejected claims 25 and 35, and include all the limitations of those claims, thereby rendering those dependent claims incomplete.

7. Claims 25-43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 25 recites the limitation "said first node" in p. 11, lines 10-11. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 35, the term "may have become untrusted" since it is unclear what may or may not constitute untrustworthiness. It is presumed that the term should read "is determined to have become untrusted."

Claims 26-34 and 36-43 depend from rejected claims 25 and 35, and include all the limitations of those claim, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1, 2, 4, and 8 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,606,668 to Shwed.

As per claim 1, Shwed discloses a computer (the engine) have a packet filter module (the data processor). Traffic is diverted to the packet filter, which tests the packet against the packet filter's rules (i.e. rules that are used to determine abnormal usage). If a rule is matched, an alert may be issued, which is sent to the computer for forwarding to the user. This is all user transparent (see column 7, lines 14-47). This system is used on a router (see column 3, lines 44-48). The monitoring of alerts is performed at the system administrator's workstation (see column 4, lines 27-42), which is a different node from the router (see figure 1).

As per claim 2, such systems inherently use memory buffers for the communications.

Regarding claim 4, the functionality is inherently performed in real-time.

Regarding claim 8, the rules are disclosed as being "security rules." Such rules are implemented to counter potential attacks.

9. Claims 20 and 22-24 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6,119,236 to Shipley et al.

As per claims 20 and 22, Shipley discloses a system for wherein several methods are disclosed for detecting abnormal usage characteristics (see column 5, line 58 to column 6, line 67). The system user-transparently then reacts by blocking all access to the LAN from a sender which is associated with a security breach (see

column 8, lines 4-9 and column 10, lines 25-27). A signal is transmitted from the INSD to the firewall via a serial connection or LAN connection; they therefore constitute separate nodes. The detecting step is performed at the INSD, while the corrective steps are performed at other nodes, such as the firewall (see column 5, lines 1-43).

As per claim 23, the process is inherently performed in real-time.

Regarding claim 24, all modern network implementations having at least the number of nodes as depicted in Figure 1 are inherently capable of supporting at least two sessions (secure or otherwise) between at least two pairs of nodes.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed as applied to claim 1 above, and further in view of U.S. Patent No. 6,119,236 to Shipley et al.

Shwed does not disclose the isolation of a network node.

Shipley, which is disclosed as being an improvement over Shwed, discloses the blocking all access to the LAN from a sender which is associated with a security breach

Art Unit: 2134

(see column 8, lines 4-9 and column 10, lines 25-27), and further notes that prior art firewalls are subject to breach by any new and unique methods of circumventing security (see column 2, lines 56-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Shwed by blocking all access to the LAN from a sender which is associated with a security breach, as disclosed by Shipley, as prior art firewalls are subject to breach by any new and unique methods of circumventing security.

11. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of U.S. Patent No. 5,737,526 to Periasamy et al.

Shwed does not discuss the hierarchical relationships among different nodes.

Periasamy discloses a hierarchically-arranged network arrangement wherein different nodes can be freely arranged among peer networks. Periasamy further discloses that this reduces broadcast traffic on slow links (see column 2, lines 49-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shwed by using a hierarchically-arranged network arrangement, as disclosed by Periasamy, to reduce broadcast traffic on slow links.

Art Unit: 2134

12. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of Kent, RFC 2401, "Security Architecture for the Internet Protocol," 1998.

Shwed does not discuss session construction within a network.

Kent discloses the construction of secure sessions in IP networks, and specifies packet information having the identification of a communicating node (see examples on p. 16), and further suggests that this allows for the enforcement of a security policy in an IP environment (see p.14).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shwed by supporting secure packet information having the identification of a communicating node, as disclosed by Kent, as this allows for the enforcement of a security policy in an IP environment.

13. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of U.S. Patent No. 6,233,704 to Scott et al.

Shwed does not discuss the remediation of node faults.

Scott discloses a system wherein remedial action by network management is triggered by a node fault. The membrane topology functions in a manner corresponding to a firewall (see column 4, line 29 to column 5, line 58). Scott further suggests that as long as faulty nodes are kept on a network, they can cause damage (see column 1, lines 47-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shwed by taking remedial action by network management in the event of a node fault, as disclosed by Scott, since as long as faulty nodes are kept on a network, they can cause damage.

14. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of U.S. Patent No. 6,301,668 to Gleichauf et al.

Shwed does not discuss the management of the various nodes.

Gleichauf discloses a system for maintaining a network map having real-time information for all nodes in a network for assessing network vulnerabilities (see column 7, lines 26-60), and further notes that can more reliably detect policy violations and patterns of misuse (see column 3, lines 7-13).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shwed by maintaining a network map, as disclosed by Gleichauf, in order to more reliably detect policy violations and patterns of misuse.

15. Claims 11-13, 15, 17, 25-28, 30, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. as applied to claim 20 above, and further in view of U.S. Patent No. 5,922,049 to Radia et al.

Regarding claims 11 and 17, the invention of Shipley disallows network access to users attempting a security breach, i.e. a potential attack (see column 8, lines 8-17); this can only be done at the point where the user enters the network (such as the router 22 in Figure 1). Shipley's exemplary configuration also only includes a single router, and describes this as a "simplified" configuration, and notes that the configuration may include "other such devices" (see column 5, lines 25-31); Shipley therefore suggests that the configuration may contain multiple routers.

Shipley does not disclose the use of locking in routers.

Radia discloses that the use of IP address locking, in order to prevent systems from forging IP addresses to fool the router into incorrectly relearning routes (see column 3, lines 5-13).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Shipley by using locking in routers, as disclosed by Radia, in order to prevent systems from forging IP addresses to fool the router into incorrectly relearning routes.

As per claim 12, Shipley discloses the use of RAM for program execution (see column 4, line 45).

Regarding claim 13, all such processing is performed in real-time.

Regarding claim 15, all modern network implementations having at least the number of nodes as depicted in Figure 1 of Shipley are inherently capable of supporting at least two sessions (secure or otherwise) between at least two pairs of nodes.

Regarding claims 25, 26, 32 nodes in the same network (including the routers and firewall) are communicatively connected. Multiple nodes (i.e. the first and second nodes) can be managed.

Regarding claim 27, 28, only the nodes that need to be controlled are controlled.

Regarding claim 30, as it is unclear what the first node actually is (see Rejection under 35 U.S.C. 112, above), this claim is being considered to stand or fall with its base claim.

16. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claim 11 above and further in view of U.S. Patent No. 5,737,526 to Periasamy et al.

Shipley and Radia do not discuss the hierarchical relationships among different nodes.

Periasamy discloses a hierarchically-arranged network arrangement wherein different nodes can be freely arranged among peer networks. Periasamy further discloses that this reduces broadcast traffic on slow links (see column 2, lines 49-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by using a hierarchically-arranged network arrangement, as disclosed by Periasamy, to reduce broadcast traffic on slow links.

17. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claim 15 above and further in view of Kent, RFC 2401, "Security Architecture for the Internet Protocol," 1998.

Shipley and Radia do not discuss session construction within a network.

Kent discloses the construction of secure sessions in IP networks, and specifies packet information having the identification of a communicating node (see examples on p. 16), and further suggests that this allows for the enforcement of a security policy in an IP environment (see p.14).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by supporting secure packet information having the identification of a communicating node, as disclosed by Kent, as this allows for the enforcement of a security policy in an IP environment.

18. Claims 18 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claims 11 and 25 above and further in view of U.S. Patent No. 6,233,704 to Scott et al.

Shipley and Radia do not discuss the remediation of node faults.

Scott discloses a system wherein remedial action by network management is triggered by a node fault. The membrane topology functions in a manner corresponding

Art Unit: 2134

to a firewall (see column 4, line 29 to column 5, line 58). Scott further suggests that as long as faulty nodes are kept on a network, they can cause damage (see column 1, lines 47-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by taking remedial action by network management in the event of a node fault, as disclosed by Scott, since as long as faulty nodes are kept on a network, they can cause damage.

19. Claims 19 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claims 11 and 35 above and further in view of U.S. Patent No. 6,301,668 to Gleichauf et al.

Shipley and Radia do not discuss the management of the various nodes.

Gleichauf discloses a system for maintaining a network map having real-time information for all nodes in a network for assessing network vulnerabilities (see column 7, lines 26-60), and further notes that can more reliably detect policy violations and patterns of misuse (see column 3, lines 7-13).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by maintaining a network map, as disclosed by Gleichauf, in order to more reliably detect policy violations and patterns of misuse.

20. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. as applied to claim 20 above, and further in view of U.S. Patent No. 6,295,276 to Datta et al.

The invention of Shipley disallows network access to users attempting a security breach (see column 8, lines 8-17); this can only be done at the point where the user enters the network (such as the router 22 in Figure 1). Shipley does not disclose routing via redundant links.

Datta discloses the use of redundant routers for network access, as it provides better fault tolerance and higher speed connections to a LAN (see abstract).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the network disclosed by Shipley to have redundant connections at access points, as it provides better fault tolerance and higher speed connections to a LAN.

Since Shipley's invention demands that a user be denied all access to a network, one skilled in the art would design the invention to disallow network access on all redundant routers in the modified configuration.

21. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claim 30 above, and further in of U.S. Patent No. 5,606,668 to Shwed.

Shipley and Radia do not disclose a human interface for supervising the system.

Art Unit: 2134

Shwed discloses a system administrator (which is inherently an authenticated user in a secure network) workstation on the network (see column 4, lines 27-42), and suggests that the invention is user by the system administrator to change the filtering or write code (see column 2, lines 5-8).

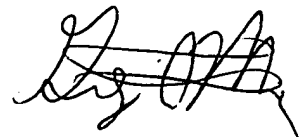
Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by having a system administrator workstation, as disclosed by Shwed, so the system administrator can change the filtering or write code.

Allowable Subject Matter

22. Claim 35 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

23. Claims 29 and 36-43 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

24. Claim 44 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 1st paragraph, set forth in this Office action.

A handwritten signature in black ink, appearing to be "D. J. [unclear]", located at the bottom right of the page.

25. Claims 45-48 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 1st paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

26. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 29, the previous cited art regarding redundant connections, Datta, only teaches to redundancy at the network edge. No art could be found that suggested redundant network connections in a secure network between hierarchically-organized nodes.

Regarding claim 35, no art could be found that isolates a node by selecting among a choice of redundant connections.

Claims 36-43 would be allowable based upon their dependence on claim 35.

Regarding claim 44, no art could be found that suggested the deployment of a manager in a network. The use of a object request broker architecture in an analogous system is suggested by U.S. Patent No. 6,393,386 to Zager et al.

Claims 45-48 would be allowable based upon their dependence on claim 44.

Response to Arguments

27. Applicant's arguments, see Remarks, filed 22 September 2005, with respect to the rejection(s) of claim(s) 1 and 20 under 35 U.S.C. 102 have been fully considered

Art Unit: 2134

and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of the same art. An explanation of the reasoning behind which Shwed and Shipley were found to anticipate some of their respective limitations was missing from the previous office action; the grounds of rejection have therefore been modified.

Conclusion

28. The grounds of rejection of the previous independent claims have been modified due to the fact that the relevant passages of Shipley and Shwed were not properly cited in the previous office action. This action is therefore non-final.

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-3800

Art Unit: 2134

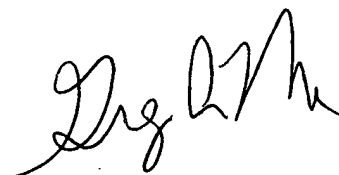
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH



December 9, 2005



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100